To: Baum, Kristina[Kristina.Baum@mail.house.gov]; McDonald, Thea[Thea.McDonald@mail.house.gov]
From: Science Space and Tech Committee Press SST Press
Sent: Thur 6/15/2017 2:14:04 PM
Subject: Vice Chairman Abraham Opening Statement- Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry

COMMITTEE ON
SCIENCE, SPACE, & TECHN
Lamar Smith, Chairman

For Immediate Release | June 15, 2017

Media Contact: Kristina Baum, Thea McDonald

Vice Chairman Abraham Opening Statement

Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry

WASHINGTON - U.S. Rep. Ralph Lee Abraham (R-La.), vice chairman of the U.S. House Science, Space, and Technology Committee's Subcommittee on Research and Technology, delivered the following opening statement today at the joint Subcommittee on Oversight and Subcommittee on Research and Technology hearing, *Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry.* Today's witness are **Mr. Salim Neino**, chief executive officer, Kryptos Logic; **Dr. Charles H. Romine**, director, Information Technology Laboratory, National Institute of Standards and Technology; **Mr. Gregory J. Touhill**, CISSP, CISM; brigadier general, USAF (ret); adjunct professor, Cybersecurity & Risk Management, Carnegie Mellon University, Heinz College; **Dr. Hugh Thompson**, chief technology officer, Symantec.

As prepared for delivery:

Thank you Mr. Chairman.

Over the last few years, we have seen an alarming increase in the number and intensity of cyber-attacks. These attacks by cyber criminals and by unfriendly governments have compromised the personal information of millions of Americans, jeopardized thousands of our businesses and their employees, and threatened interruption of critical public services. The recent WannaCry ransomware attack demonstrates that cyber-attacks are continuing to go from bad to worse.

This most recent large-scale cyber attack affected more than one to two million systems in more than 190 countries. Nevertheless, it appears that the impact could have been much more catastrophic considering how fast this ransomware spread.

While organizations and individuals within the United States were largely unscathed, due in part to a security researcher identifying a web-based "kill switch," the potential destructiveness of WannaCry warns us to expect similar attacks in the future. Before those attacks happen, we need to make sure that our information systems are ready.

During a Research and Technology Subcommittee hearing earlier this year, a witness representing the U.S. Government Accountability Office (GAO) testified that, "Over the past several years, GAO has made about 2,500 recommendations to federal agencies to enhance their information security programs and controls. As of February 2017, about 1,000 recommendations had not been implemented."

It is clear that the status quo in federal government cyber security is a virtual invitation for more cyber-attacks. We must take strong steps in order to properly secure our systems and databases before another cyber-attack like WannaCry literally puts our government up for ransom.

On March 1, 2017, this Committee approved H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, a bill that I introduced as part of my ongoing interest over the state of our nation's cybersecurity.

This bill takes concrete steps to help strengthen Federal government cybersecurity. The most important steps are encouraging federal agencies to adopt the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, which is used by many private businesses, and directing NIST to initiate individual cybersecurity audits of priority Federal agencies to determine the extent to which each agency is meeting the information security standards

developed by the Institute.

NIST's in-house experts develop government-wide technical standards and guidelines under the Federal Information Security Modernization Act of 2014. And NIST experts also developed, through collaborations between government and private sector, the Framework for Improving Critical Infrastructure Cybersecurity that federal agencies are now required to use pursuant to the President's recent Cybersecurity Executive Order. I was very pleased to read that language.

Considering the growing attempts to infiltrate information systems, there is an urgent need to assure Americans that all federal agencies are doing everything that they can to protect government networks and sensitive data. The status quo simply isn't working. We can't put up with more bureaucratic excuses and delays.

NIST's cyber expertise is a singular asset. We should take full advantage of that asset, starting with the very important step of annual NIST cyber audits of high priority federal agencies.

As cyber-attacks and cyber criminals continue to evolve and become more sophisticated, our government's cyber defenses must adapt, too, in order to protect vital public services and shield hundreds of millions of Americans' confidential information.

We will hear from our witnesses today about lessons learned from the WannaCry attack and how the government can bolster the security of its systems. We must keep in mind that the next cyber attack is just around the corner, and it could have a far greater impact than what we have seen thus far.

Our government systems need to be better protected, and that starts with more accountability, responsibility, and transparency by federal agencies.

Thank you and I look forward to hearing from our panel.

###

www.science.house.gov

--